

JP10240500

Publication Title:

**RANDOM NUMBER GENERATOR AND METHOD, ENCIPHERING DEVICE
AND METHOD, DECODER AND METHOD AND STREAM CIPHER SYSTEM**

Abstract:

PROBLEM TO BE SOLVED: To obtain a random number generator whose linear complexity is large in comparison with a device scale and which is also cryptographically secure by sequentially changing a 1st random number series that is generated based on a 2nd random number series that is generated.

SOLUTION: This device is provided with a 1st random number generating part 2, a 2nd random number generating part 4 and a random number converting part 6. The part 2 generates random number series (binary series) and outputs it after it is set to an initial state. Similarly, the part 4 generates random number series (binary series) and outputs it after it is set to an initial state. The part 6 switches orders of inputted binary series based on binary series that are differently inputted and outputs them. Random number series (a) which are outputted from the part 2 are inputted to the part 6, and the part 6 switches the orders of the random number series (a) which are outputted from the part 2 through the procedure or operation based on random number series (b) which are outputted from the part 4 and outputs them.

Data supplied from the esp@cenet database - <http://ep.espacenet.com>

This Patent PDF Generated by Patent Fetcher(TM), a service of Patent Logistics, LLC

Patent provided by Sughrue Mion, PLLC - <http://www.sughrue.com>

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-240500

(43)公開日 平成10年(1998)9月11日

(51)Int.Cl.⁶
G 0 6 F 7/58
G 0 9 C 1/00
識別記号
6 5 0

F I
G 0 6 F 7/58
G 0 9 C 1/00
A
B
6 5 0 B

審査請求 未請求 請求項の数15 O L (全 16 頁)

(21)出願番号 特願平9-45954
(22)出願日 平成9年(1997)2月28日

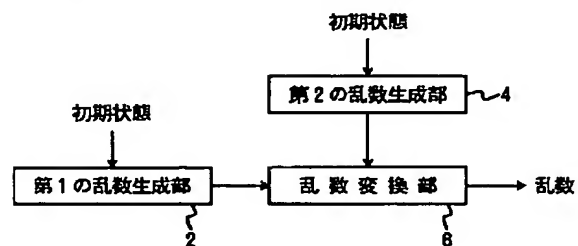
(71)出願人 000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者 清水 秀夫
神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内
(72)発明者 川村 信一
神奈川県川崎市幸区小向東芝町1番地 株
式会社東芝研究開発センター内
(74)代理人 弁理士 鈴江 武彦 (外6名)

(54)【発明の名称】 乱数生成装置及び方法、暗号化装置及び方法、復号装置及び方法、並びにストリーム暗号システム

(57)【要約】

【課題】 装置規模に比して線形複雑度が大きく暗号的にも安全な乱数生成装置を提供すること。

【解決手段】 所定の初期状態をもとに第1の乱数系列を生成する手段と、所定の初期状態をもとに第2の乱数系列を生成する手段と、第1の乱数系列を、第2の乱数系列に基づいて順序変更する手段を備える。また、所定の初期状態をもとに第1の乱数系列を所定ビット長単位に生成する第1の線形フィードバックシフトレジスタと、所定の初期状態をもとに第2の乱数系列を所定ビット長単位に生成する第2の線形フィードバックシフトレジスタと、第2の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数にて示されるアドレスに格納されている内容を出力した後に該アドレスに第1の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数を格納する記憶装置を備える。



【特許請求の範囲】

【請求項1】所定の初期状態をもとに第1の乱数系列を生成する第1の乱数生成手段と、

所定の初期状態をもとに第2の乱数系列を生成する第2の乱数生成手段と、

生成された前記第1の乱数系列を、生成された前記第2の乱数系列に基づいて順序変更する変換手段とを備えたことを特徴とする乱数生成装置。

【請求項2】所定の初期状態をもとに第1の乱数系列を所定のビット長単位に生成する第1の線形フィードバックシフトレジスタと、

所定の初期状態をもとに第2の乱数系列を所定のビット長単位に生成する第2の線形フィードバックシフトレジスタと、

前記第2の線形フィードバックシフトレジスタから与えられた前記所定のビット長の乱数にて示されるアドレスに格納されている内容を読み出した後に、該アドレスに前記第1の線形フィードバックシフトレジスタから与えられた前記所定のビット長の乱数を格納する記憶装置とを備えたことを特徴とする乱数生成装置。

【請求項3】所定の初期状態をもとに2値乱数を順次出力する第1の線形フィードバックシフトレジスタと、

所定の初期状態をもとに2値乱数を順次出力する第2の線形フィードバックシフトレジスタと、

前記第2の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数にて示されるアドレスに格納されている内容を読み出した後に、該アドレスに前記第1の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数を格納する第1の記憶装置と、

前記第1の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数にて示されるアドレスに格納されている内容を読み出した後に、該アドレスに前記第2の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数を格納する第2の記憶装置と、

前記第1の記憶装置から出力された所定のビット長の乱数と前記第2の記憶装置から出力された所定のビット長の乱数とを入力とする非線形変換処理を行って所定のビット長の乱数を生成して出力する非線形コンバイナとを備えたことを特徴とする乱数生成装置。

【請求項4】所定の初期状態をもとに生成した第1の乱数系列を、所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して出力することを特徴とする乱数生成方法。

【請求項5】所定の初期状態をもとに第1の乱数系列を生成する第1の線形フィードバックシフトレジスタにより所定のビット長の乱数を所定個数生成し、生成された前記乱数夫々を、記憶装置の各アドレスの内容として格納し、

所定の初期状態をもとに第2の乱数系列を生成する第2の線形フィードバックシフトレジスタにより生成された

所定のビット長の乱数にて示される前記記憶装置のアドレスに格納されている内容を乱数として出力し、

この内容を出力された前記記憶装置のアドレスに、前記第1の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数を格納し、

以降、前記記憶装置から出力された乱数系列が所定の長さになるまで、前記記憶装置からの乱数の出力と前記記憶装置への乱数の格納を繰り返して実行することを特徴とする乱数生成方法。

【請求項6】所定の初期状態をもとに第1の乱数系列を生成する第1の線形フィードバックシフトレジスタにより所定のビット長の乱数を所定個数生成し、生成された前記乱数夫々を、第1の記憶装置の各アドレスの内容として格納するとともに、所定の初期状態をもとに第2の乱数系列を生成する第2の線形フィードバックシフトレジスタにより所定のビット長の乱数を所定個数生成し、生成された前記乱数夫々を、第2の記憶装置の各アドレスの内容として格納し、

前記第2の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数にて示される前記第1の記憶装置のアドレスに格納されている内容を読み出して2入力1出力の非線形コンバイナに与えたとともに、前記第1の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数にて示される前記第2の記憶装置のアドレスに格納されている内容を読み出して前記非線形コンバイナに与え、この非線形コンバイナにより非線形変換処理を行って所定のビット長の乱数を生成して出力し、

前記第1の記憶装置の前記内容の出力されたアドレスに、前記第1の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数を格納するとともに、前記第2の記憶装置の前記内容の出力されたアドレスに、前記第2の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数を格納し、

以降、前記非線形コンバイナから出力された乱数系列が所定の長さになるまで、前記第1および第2の記憶装置からの乱数の出力をもとにした非線形変換処理と前記第1および第2の記憶装置への乱数の格納を繰り返して実行することを特徴とする乱数生成方法。

【請求項7】共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、

平文および暗号文の一方の2値系列と前記鍵系列とをもとに予め定められた論理演算を行って平文および暗号文の他方の2値系列を生成する論理演算手段とを備えたことを特徴とする暗号処理装置。

【請求項8】前記論理演算手段は、ビット単位の排他的論理和演算を行うものであることを特徴とする請求項7

に記載の暗号処理装置。

【請求項9】共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力し、平文および暗号文の一方の2値系列と前記鍵系列とをもとに予め定められた論理演算を行って平文および暗号文の他方の2値系列を生成することを特徴とする暗号処理方法。

【請求項10】共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、

平文の2値系列と前記鍵系列とをもとに予め定められた論理演算を行って暗号文の2値系列を生成する論理演算手段とを備えたことを特徴とする暗号化装置。

【請求項11】共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力し、

平文の2値系列と前記鍵系列とをもとに予め定められた論理演算を行って暗号文の2値系列を生成することを特徴とする暗号化方法。

【請求項12】共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、

暗号文の2値系列と前記鍵系列とをもとに予め定められた論理演算を行ってもとの平文の2値系列を生成する論理演算手段とを備えたことを特徴とする復号装置。

【請求項13】共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力し、

暗号文の2値系列と前記鍵系列とをもとに予め定められた論理演算を行ってもとの平文の2値系列を生成することを特徴とする復号方法。

【請求項14】所定の共通鍵をもとに平文を暗号文に変換する暗号化装置と該所定の共通鍵をもとに暗号文をもとの平文に変換する復号装置と該暗号化装置から該復号装置へ暗号文を伝える所定の媒体とを備えたストリーム暗号システムにおいて、

前記暗号化装置は、

共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、

平文の2値系列と前記鍵系列とをもとに予め定められた

論理演算を行って暗号文の2値系列を生成する論理演算手段とを備え、

前記復号装置は、

共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力する、前記乱数生成手段と同一の論理構造を持つ乱数生成手段と、

暗号文の2値系列と前記鍵系列とをもとに前記論理演算と同一の論理演算を行ってもとの平文の2値系列を生成する論理演算手段とを備えたことを特徴とするストリーム暗号システム。

【請求項15】一方の処理装置にて所定の共通鍵をもとに平文を暗号文に変換し、該暗号文を所定の媒体に出力し、他方の処理装置にて該暗号文を該所定の媒体を通じて入力し、該所定の共通鍵をもとに暗号文をもとの平文に変換するストリーム暗号システムにおいて、

前記処理装置は、

共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、

平文および暗号文の一方の2値系列と前記鍵系列とをもとに予め定められた論理演算を行って平文および暗号文の他方の2値系列を生成する論理演算手段とを備えたことを特徴とするストリーム暗号システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、簡易な構成でかつ暗号に使用しても安全な乱数生成装置及び方法、その疑似乱数生成器を用いた暗号化装置及び方法、復号装置及び方法、並びにストリーム暗号システムに関する。

【0002】

【従来の技術】現在、暗号方式として様々なものが知られているが、その1つに加算型ストリーム暗号がある。加算型ストリーム暗号は、良く知られているように、暗号側と復号側で同一または同一の論理構造の疑似乱数生成器を持ち、暗号側では平文メッセージと共通鍵にて示される初期状態にセットされた疑似乱数生成器から出力される乱数系列（鍵系列）とをビット単位に足し込む（排他的論理和が良く用いられる）ことで暗号化を行い、復号側ではこの暗号化されたメッセージを入力として暗号側と同一の手順を実行することにより復号化を行うものである。

【0003】このような加算型ストリーム暗号のなかでも、M系列を出力する線形フィードバックシフトレジスタを疑似乱数生成器として利用する構成は、装置規模が小さくなることもあり、良く用いられている。図13に線形フィードバックシフトレジスタの原理図を示す。図中の $C_1 \sim C_n$ は予め0または1に定められ、n段のシ

フトレジスタ S_{i-k} の値のうち $C_k = 1$ であるものの排他的論理和が出力 S_i になり、シフト動作においてこの S_i がフィードバックされる。また、線形フィードバックシフトレジスタをセットする初期状態が共通鍵となる。

【0004】しかしながら、線形フィードバックシフトレジスタ自体は、レジスタ長の2倍の出力を観測することで、その構造と初期状態のすべてを特定することが可能なので、加算型ストリーム暗号に用いる疑似乱数生成器としては、安全性に関して問題がある。また、線形フィードバックレジスタを疑似乱数生成器として用いるために、レジスタ長を長くして安全性を高めようとすることは、装置規模の点から問題がある。

【0005】そこで、複数の線形フィードバックシフトレジスタの出力を非線形コンバイナで結合する手法や、線形フィードバックシフトレジスタの出力に非線形変換を施す手法等が開発されている（例えば文献1「暗号理論入門」、共立出版株式会社、岡本栄司著、1993年発行などに詳しい）。

【0006】しかし、複数の線形フィードバックシフトレジスタの出力を非線形コンバイナで結合する方式では、線形複雑度はたかだか各線形フィードバックシフトレジスタのレジスタ長の積程度にしかない。

【0007】ここで、線形複雑度は、疑似乱数生成器の解読しずらさ、すなわち暗号学的な安全性を計るための尺度として用いられる指標で、「ある初期値から始めれば同じ出力と同じ周期をもつという意味で等価な線形フィードバックシフトレジスタのレジスタ長」と定義される（文献1参照）。

【0008】そこで、装置規模に比して線形複雑度が大きくなる疑似乱数生成器があれば、経済的にも安全性の観点からも非常に都合が良い。そのような疑似乱数生成器の候補として、加算ジェネレータ（summation generator；例えば文献2“APPLIED CRYPTOGRAPHY”、John Wiley & Sons, Inc. 社、1996年発行、p. 386～387に詳しい）が提案された。図14に加算ジェネレータの一例を示す。この場合、シフトレジスタ b_1 と b_2 とキャリアの和を2で割った剰余をシフトレジスタにフィードバックするとともに、 b_1 と b_2 とキャリアの和を2で割った商を新たなキャリアとして保持する動作を繰り返す。

【0009】ところが、加算ジェネレータの線形複雑度は線形フィードバックシフトレジスタのレジスタ長の指数程度となることが知られているが、加算ジェネレータは既に解読されており、加算型ストリーム暗号に用いる疑似乱数生成器としては、安全性に関して問題がある。

【0010】

【発明が解決しようとする課題】以上説明したように、従来、小さな装置規模で安全性の高いストリーム暗号を

実現し得る線形複雑度の大きな乱数生成装置は知られていなかった。本発明は、上記事情を考慮してなされたもので、装置規模に比して線形複雑度が大きく暗号的にも安全な乱数生成装置及び方法、暗号化装置及び方法、復号装置及び方法、並びにストリーム暗号システムを提供することを目的とする。

【0011】

【課題を解決するための手段】本発明（請求項1）に係る乱数生成装置は、所定の初期状態をもとに第1の乱数系列を生成する第1の乱数生成手段と、所定の初期状態をもとに第2の乱数系列を生成する第2の乱数生成手段と、生成された前記第1の乱数系列を、生成された前記第2の乱数系列に基づいて順序変更する変換手段とを備えたことを特徴とする。

【0012】本発明（請求項2）に係る乱数生成装置は、所定の初期状態をもとに第1の乱数系列を所定のビット長単位に生成する第1の線形フィードバックシフトレジスタと、所定の初期状態をもとに第2の乱数系列を所定のビット長単位に生成する第2の線形フィードバックシフトレジスタと、前記第2の線形フィードバックシフトレジスタから与えられた前記所定のビット長の乱数にて示されるアドレスに格納されている内容を出力した後に、該アドレスに前記第1の線形フィードバックシフトレジスタから与えられた前記所定のビット長の乱数を格納する記憶装置とを備えたことを特徴とする。

【0013】なお、1つの線形フィードバックシフトレジスタのみ設け、これを第1の線形フィードバックシフトレジスタおよび第2の線形フィードバックシフトレジスタとして用いても良い。

【0014】また、一部または全部の線形フィードバックシフトレジスタを、他の公知の乱数生成器に置き換えても良い。本発明（請求項3）に係る乱数生成装置は、所定の初期状態をもとに2値乱数を順次出力する第1の線形フィードバックシフトレジスタと、所定の初期状態をもとに2値乱数を順次出力する第2の線形フィードバックシフトレジスタと、前記第2の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数にて示されるアドレスに格納されている内容を出力した後に、該アドレスに前記第1の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数を格納する第1の記憶装置と、前記第1の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数にて示されるアドレスに格納されている内容を出力した後に、該アドレスに前記第2の線形フィードバックシフトレジスタから与えられた所定のビット長の乱数を格納する第2の記憶装置と、前記第1の記憶装置から出力された所定のビット長の乱数と前記第2の記憶装置から出力された所定のビット長の乱数とを入力とする非線形変換処理を行って所定のビット長の乱数を生成して出力する非線形コンバイナとを備えたことを特徴とする。

【0015】なお、第1の線形フィードバックシフトレジスタを記憶装置に格納するデータ用と記憶装置に与えるアドレス用で共用する代わりに、データ専用とアドレス専用の2つの線形フィードバックシフトレジスタを設けても良い。同様に、第2の線形フィードバックシフトレジスタも共用する代わりに、データ専用とアドレス専用の2つの線形フィードバックシフトレジスタを設けても良い。

【0016】また、一部または全部の線形フィードバックシフトレジスタを、他の公知の乱数生成器に置き換えても良い。本発明に係る乱数生成装置における一部または全部の線形フィードバックシフトレジスタを、本発明に係る乱数生成装置自体で置き換えても良い。この置き換えは、何階層に渡って行っても良い。

【0017】本発明（請求項4）に係る乱数生成方法は、所定の初期状態をもとに生成した第1の乱数系列を、所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して出力することを特徴とする。

【0018】本発明（請求項5）に係る乱数生成方法は、所定の初期状態をもとに第1の乱数系列を生成する第1の線形フィードバックシフトレジスタにより所定のビット長の乱数を所定個数生成し、生成された前記乱数夫々を、記憶装置の各アドレスの内容として格納し、所定の初期状態をもとに第2の乱数系列を生成する第2の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数にて示される前記記憶装置のアドレスに格納されている内容を乱数として出力し、この内容を出力された前記記憶装置のアドレスに、前記第1の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数を格納し、以降、前記記憶装置から出力された乱数系列が所定の長さに達するまで、前記記憶装置からの乱数の出力と前記記憶装置への乱数の格納を繰り返し実行することを特徴とする。

【0019】本発明（請求項6）に係る乱数生成方法は、所定の初期状態をもとに第1の乱数系列を生成する第1の線形フィードバックシフトレジスタにより所定のビット長の乱数を所定個数生成し、生成された前記乱数夫々を、第1の記憶装置の各アドレスの内容として格納するとともに、所定の初期状態をもとに第2の乱数系列を生成する第2の線形フィードバックシフトレジスタにより所定のビット長の乱数を所定個数生成し、生成された前記乱数夫々を、第2の記憶装置の各アドレスの内容として格納し、前記第2の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数にて示される前記第1の記憶装置のアドレスに格納されている内容を出力して2入力1出力の非線形コンバイナに与えるとともに、前記第1の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数にて示される前記第2の記憶装置のアドレスに格納されている内容を出力して前記非線形コンバイナに与え、この非線形コン

バイナにより非線形変換処理を行って所定のビット長の乱数を生成して出力し、前記第1の記憶装置の前記内容の出力されたアドレスに、前記第1の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数を格納するとともに、前記第2の記憶装置の前記内容の出力されたアドレスに、前記第2の線形フィードバックシフトレジスタにより生成された所定のビット長の乱数を格納し、以降、前記非線形コンバイナから出力された乱数系列が所定の長さに達するまで、前記第1および第2の記憶装置からの乱数の出力をもとにした非線形変換処理と前記第1および第2の記憶装置への乱数の格納を繰り返し実行することを特徴とする。

【0020】本発明（請求項7）に係る暗号処理装置は、共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、平文および暗号文の一方の2値系列と前記鍵系列とをもとに予め定められた論理演算を行って平文および暗号文の他方の2値系列を生成する論理演算手段とを備えたことを特徴とする。

【0021】本発明（請求項9）に係る暗号処理方法は、共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力し、平文および暗号文の一方の2値系列と前記鍵系列とをもとに予め定められた論理演算を行って平文および暗号文の他方の2値系列を生成することを特徴とする。

【0022】本発明（請求項10）に係る暗号化装置は、共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、平文の2値系列と前記鍵系列とをもとに予め定められた論理演算を行って暗号文の2値系列を生成する論理演算手段とを備えたことを特徴とする。

【0023】本発明（請求項11）に係る暗号化方法は、共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力し、平文の2値系列と前記鍵系列とをもとに予め定められた論理演算を行って暗号文の2値系列を生成することを特徴とする。

【0024】本発明（請求項12）に係る復号装置は、共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、暗号文の2値系列と前記鍵系列とをもとに予め定められた論

理演算を行ってもとの平文の2値系列を生成する論理演算手段とを備えたことを特徴とする。

【0025】本発明(請求項13)に係る復号方法は、共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力し、暗号文の2値系列と前記鍵系列とをもとに予め定められた論理演算を行ってもとの平文の2値系列を生成することを特徴とする。

【0026】本発明(請求項14)は、所定の共通鍵をもとに平文を暗号文に変換する暗号化装置と該所定の共通鍵をもとに暗号文をもとの平文に変換する復号装置と該暗号化装置から該復号装置へ暗号文を伝える所定の媒体とを備えたストリーム暗号システムにおいて、前記暗号化装置は、共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、平文の2値系列と前記鍵系列とをもとに予め定められた論理演算を行って暗号文の2値系列を生成する論理演算手段とを備え、前記復号装置は、共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力する、前記乱数生成手段と同一の論理構造を持つ乱数生成手段と、暗号文の2値系列と前記鍵系列とをもとに前記論理演算と同一の論理演算を行ってもとの平文の2値系列を生成する論理演算手段とを備えたことを特徴とする。

【0027】本発明(請求項15)は、一方の処理装置にて所定の共通鍵をもとに平文を暗号文に変換し、該暗号文を所定の媒体に出力し、他方の処理装置にて該暗号文を該所定の媒体を通じて入力し、該所定の共通鍵をもとに暗号文をもとの平文に変換するストリーム暗号システムにおいて、前記処理装置は、共通鍵により与えられる所定の初期状態をもとに生成した第1の乱数系列を、共通鍵により与えられる所定の初期状態をもとに生成した第2の乱数系列に基づいて順序変更して、鍵系列として出力する乱数生成手段と、平文および暗号文の一方の2値系列と前記鍵系列とをもとに予め定められた論理演算を行って平文および暗号文の他方の2値系列を生成する論理演算手段とを備えたことを特徴とする。

【0028】本発明における論理演算は、例えば、ビット単位の排他的論理和演算である。なお、本発明の暗号処理、暗号装置、復号装置の乱数生成手段には、請求項2の乱数生成装置や請求項3の乱数生成装置や上述したようにこれらを変形したものを適用することもできる。

【0029】本発明では、記憶装置を緩衝域として用い、第1の線形フィードバックシフトレジスタAの出力を該記憶装置のアドレスとして入力し、該アドレスに記

憶されている内容を乱数として出力し、該アドレスに第2の線形フィードバックシフトレジスタBの出力をデータ入力として記憶することで、線形複雑度の大きな乱数生成装置を実現することができる。

【0030】線形フィードバックシフトレジスタAとBのレジスタ長を各々 L_A 、 L_B とする。請求項2等に係る発明のように記憶装置を緩衝域として用いる乱数生成装置での線形複雑度は、ほぼ $L_A \times 2^{L_B}$ である。

【0031】請求項3等に係る発明の2つの記憶装置を互いの緩衝域として用いる乱数生成器での線形複雑度は、ほぼ $2^{L_A} \times 2^{L_B}$ である。また、乱数生成装置を用いるストリーム暗号では、暗号の解読しづらさという意味での安全性を計るための尺度として、線形複雑度が用いられる。つまり、線形装置規模に比して線形複雑度が大きいことは、安価に安全な暗号装置を構築できることを意味する。

【0032】このように本発明によれば、少ない装置規模で大きな線形複雑度を達成できるので、経済的に安全な暗号を実現できる。なお、上記の発明は、相当する手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体としても成立する。

【0033】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。本発明に係る乱数生成装置および方法は、装置規模に比して大きな線形複雑度を得ることができるものであり、もちろん乱数を必要とする種々の分野に適用可能であるが、特に、統計的性質だけでなく予測可能性、端的に言えばアタックに対する安全性をも問題とされる暗号、中でもストリーム暗号に好適なものである。

【0034】最初に、本発明の乱数生成装置および方法の基本的な考え方について説明する。図1に、本発明の一実施形態に係る乱数生成装置の構成を示す。

【0035】本乱数生成装置は、第1の乱数生成部2と、第2の乱数生成部4と、乱数変換部6を備えている。第1の乱数生成部2は、初期状態にセットされた後、乱数系列(2値系列)aを生成し出力していく。

【0036】同様に、第2の乱数生成部4は、初期状態にセットされた後、乱数系列(2値系列)bを生成し出力していく。なお、第1の乱数生成部2は、初期状態が同一であれば、同一の乱数系列を生成する。第2の乱数生成部4についても同様である。また、第1の乱数生成部2や第2の乱数生成部4についての初期状態とは、例えば内部変数あるいは各レジスタの保持する値の初期値群であり、例えば線形フィードバックシフトレジスタにおける各シフトレジスタの保持する初期値の組がこれに該当する。

【0037】また、第1の乱数生成部2の初期状態と第2の乱数生成部4の初期状態は独立のものであるが、第

1の乱数生成部2と第2の乱数生成部4が同様の構成の場合に同一のものを使用しても構わない。

【0038】乱数変換部6は、入力された2値系列の順序を、別に入力された2値系列に基づいて入れ替えて出力する。また、2値系列の順序の入れ替えは、連続する所定のビット数（1ビットの場合を含む）を一纏まりとして行われる。

【0039】入れ替えの方法は、乱数変換部6は、入力された2値系列aの順序を、別に入力された2値系列bに基づいて入れ替えて出力する。2値系列aの順序の入れ替えは、連続する所定のビット数（1ビットの場合を含む）を一纏まりとして行われる。例えば、連続する64ビットを一纏まりとする。

【0040】2値系列aの順序の入れ替えの方法は、例えば、上記の別に入力された2値系列bを連続するnビット（例えば8ビット）ごとに区切って得た2進数nビットの情報の系列に従って、2値系列a中のある位置の一纏まりを他の位置（結果的に同じ位置になる場合を含む）に移す。

【0041】2値系列aが同一でも、2値系列bが相違すれば、乱数変換部6の出力として得られる乱数系列は相違するものとなる。また、第1の乱数生成部2の初期状態と第2の乱数生成部4の初期状態の組が同一であれば、乱数変換部6の出力として得られる乱数系列は同一になる。

【0042】詳しくは後述するが、この乱数変換部6は、例えばRAMなどの記憶装置を用いることにより実現することが可能である。図1において、第1の乱数生成部2から出力された乱数系列aが乱数変換部6に入力され、乱数変換部6では第2の乱数生成部4から出力された乱数系列bに基づいた手順または動作で、第1の乱数生成部2から出力された乱数系列aの順序を入れ替えて出力する。

【0043】例えば、乱数系列aが $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, \dots$ (a_i は0または1)で、乱数変換部6は連続する2ビットを一纏まりとして順序の入れ替えを行う場合、乱数変換部6から出力される乱数系列は、乱数系列bの内容に応じて、 $a_3, a_4, a_7, a_8, a_1, a_2, \dots$ 、あるいは $a_5, a_6, a_1, a_2, a_7, a_8, \dots$ などとなる。

【0044】なお、図1の乱数生成装置の他の例として、第1の乱数生成部2と第2の乱数生成部4とを1つに共通化しても良い。この場合、第1の乱数生成部2として所定のビット数の乱数を生成する動作と、第2の乱数生成部4として所定のビット数の乱数を生成する動作とを交互に行えば良い。言い換えると、この共通化された乱数生成装置から出力される乱数系列を、上記の2値系列a用と2値系列b用に交互に使えば良い。

【0045】また、図1の乱数生成装置のさらに他の例として、図1の乱数生成装置における第1の乱数生成部

2および第2の乱数生成部4の少なくとも一方を、図1の乱数生成装置自体で置き換えた構成にしても良い。

【0046】次に、本発明の乱数生成装置をストリーム暗号に適用する場合について説明する。ストリーム暗号では、暗号側において、平文メッセージ（2値系列）と所定の共通鍵に基づいて生成された鍵系列（2値系列）にビット単位の所定の論理演算（一般的には排他的論理和演算）を施して暗号文を生成し、復号側において、暗号文（2値系列）と所定の共通鍵（暗号側で使った鍵と同一のもの）に基づいて生成された暗号側と同一の鍵系列にビット単位の所定の論理演算（暗号側で使った演算と同一のもの）を施してもとの平文メッセージを得る。

【0047】このようなストリーム暗号において、上記の鍵系列を生成する装置として、前述したまたは後述する本実施形態の乱数生成装置を用いると効果的である。この場合、乱数生成装置の初期状態は、共通鍵として与えられるようにする。

【0048】図2に、本発明の乱数生成装置をストリーム暗号に適用した暗号システムの構成例を示す。暗号側（例えばデータを伝える媒体に通信路を用いる場合の送信側）の暗号装置には、本実施形態の乱数生成装置10aと、論理演算処理装置12aが備えられている。

【0049】同様に、復号側（例えばデータを伝える媒体に通信路を用いる場合の受信側）の復号装置には、本実施形態の乱数生成装置10bと、論理演算処理装置12bが備えられている。

【0050】乱数生成装置10aと乱数生成装置10bとは同一または同一の論理構造を持つものであり、論理演算処理装置12aと論理演算処理装置12bとは同一または等価なものである。なお、ここでは、論理演算処理装置12aと論理演算処理装置12bは、ビット単位の排他的論理和演算を行うものとして説明する。

【0051】図2において、暗号側と復号側との間では、何らかの公知の方法で共通鍵を共有しているものとする。この共通鍵により、乱数生成装置10aおよび11の初期状態が与えられる。共通鍵の内容は、乱数生成装置10aおよび11の初期状態そのものであっても良いし、初期状態を特定可能な識別子でも良い。

【0052】そして、暗号側では、暗号化したい平文メッセージと、所定の共通鍵により与えられる初期状態をもとにした乱数生成装置10aの生成する乱数系列との排他的論理和を取って、平文メッセージを暗号文に変換し、通信路等を介して暗号側に伝える。

【0053】暗号文を取得した復号側では、この暗号文と、前記共通鍵により与えられる初期状態をもとにした乱数生成装置10bの生成する乱数系列との排他的論理和を取ることで、もとの平文メッセージを復元する。

【0054】たとえ不正な盗聴者がたとえ暗号文を入手したとしても、共通鍵を知らないので、平文を復元する

ことはできない。なお、暗号側から復号側に暗号文を渡すための手段はどのようなものであっても構わない。例えば、両者をネットワークで接続する方法、無線通信により暗号文を伝送する方法、暗号文を可搬できる記憶媒体に格納して受け渡す方法など種々のものが考えられる。なお、これらに対応する機能部分は、図2においては省略されている。

【0055】また、暗号装置と復号装置で行う処理は実質的に同じであるので、実際には、計算機などの処理装置は、暗号装置と復号装置の両方の機能を持つことができる。

【0056】以下では、本発明の実施の形態に係る乱数生成装置についてより詳しく説明していく。図3に、本発明の一実施形態に係る乱数生成装置の構成を示す。また、図4に、本乱数生成装置の動作の流れを示す。

【0057】本乱数生成装置は、第1の線形フィードバックシフトレジスタ20、第2の線形フィードバックシフトレジスタ22、記憶装置24を備えている。第1の線形フィードバックシフトレジスタ20および第2の線形フィードバックシフトレジスタ22夫々の内部基本構成は、既に説明した図13と同様のものを用いることができる。

【0058】第1の線形フィードバックシフトレジスタ20と第2の線形フィードバックシフトレジスタ22のシフトレジスタ数は、独立に設定することができる。同数でも良いし、異なる数でも良い。また、シフトレジスタ数が同数である場合に、第1の線形フィードバックシフトレジスタ20と第2の線形フィードバックシフトレジスタ22の内部構造は、独立に設定することができ、同一構造でも異なる構造でも良い。

【0059】なお、線形フィードバックシフトレジスタ20、22夫々の生成多項式は最大長系列を出力させるために既約多項式であることが望ましい。また、第1の乱数生成部2にセットする初期状態と第2の乱数生成部4にセットする初期状態は独立のものであるが、第1の線形フィードバックシフトレジスタ20と第2の線形フィードバックシフトレジスタ22のシフトレジスタ数が同一の場合に、両者の初期状態を同一にしても構わない。

【0060】上記のような第1の線形フィードバックシフトレジスタ20は、初期状態にセットされた後、乱数系列(2値系列)Dを所定のビット単位(例えば64ビット単位)に生成し出力していく。この単位となるビット数をu1で表す。

【0061】同様に、第2の乱数生成部4は、初期状態にセットされた後、乱数系列(2値系列)Aを所定のビット単位(例えば8ビット単位)に生成し出力していく。この単位となるビット数をu2で表す。

【0062】記憶装置24は、例えばRAMなどのように指定したアドレスに対する書き込みおよび読み出しが

可能な記憶素子を用いて構成される。記憶装置24は、少なくとも 2^{u2} ($=m$)種類のアドレスの夫々にu1ビットのデータを格納できる容量を持つものとする。ただし、記憶装置24は、1つの記憶素子から構成されていても複数の記憶素子から構成されていても構わない。

【0063】第1の線形フィードバックシフトレジスタ20から逐次出力されるu1ビットの乱数は、記憶装置24にデータ入力として与えられる。一方、第2の線形フィードバックシフトレジスタ22から逐次出力されるu2ビットの乱数は、記憶装置24にアドレス入力として与えられる。

【0064】なお、第2の線形フィードバックシフトレジスタ22から出力されるu2ビットの乱数が直接、記憶装置24のアドレスを示すものとしても良いし、間接的に、該乱数により記憶装置24のアドレスが特定されるようにしても良い。例えば、u2=4で乱数が“1001”の場合に記憶装置24のアドレス“1001”が示されるようにしても良いし、例えば定数+乱数×4などのアドレス変換式あるいは予め設定されたアドレス変換テーブルにより実際のアドレスが示されるものとしても良い。

【0065】なお、第2の線形フィードバックシフトレジスタ22から出力されるu2ビットの乱数により、間接的に記憶装置24のアドレスが特定されるようにする場合における、乱数をアドレスに変換する機能部分については図示を省略した。

【0066】次に、図4を参照しながら本乱数生成装置の動作について説明する。まず、初期処理として、第1の線形フィードバックシフトレジスタ20および第2の線形フィードバックシフトレジスタ22夫々を所望の初期状態にセットする(ステップS1)。

【0067】そして、第1の線形フィードバックシフトレジスタ20によりu1ビットの乱数をm個生成し、これらを記憶装置24のm種類のアドレス(例えば0~m-1番地)に夫々格納する(ステップS2)。

【0068】m個の乱数夫々をどのアドレスに格納するかは種々の方法が考えられるが、例えば、生成された順番に0番地~m-1番地へと格納していく。次に、第2の線形フィードバックシフトレジスタ22によりu2ビットの乱数を1つ生成する(ステップS3)。

【0069】そして、記憶装置24のアドレスのうち、ステップS3で生成された乱数にて示されるアドレスの内容(u1ビットの2値データ)を出力する(ステップS4)。

【0070】この時点で、生成すべき乱数系列のうち最初のu1ビットのデータが得られたことになる。次に、第1の線形フィードバックシフトレジスタ20によりu1ビットの乱数を1つ生成する(ステップS6)。

【0071】そして、記憶装置24のアドレスのうち、ステップS4で内容の出力されたアドレスに、ステップ

S5で生成された乱数を格納する(ステップS7)。次に、ステップS3に戻って第2の線形フィードバックシフトレジスタ22によりu2ビットの乱数を1つ生成する(ステップS3)。

【0072】そして、記憶装置24のアドレスのうち、ステップS3で生成された乱数にて示されるアドレスの内容(u1ビットの2値データ)を出力する(ステップS4)。

【0073】この時点で、生成すべき乱数系列のうち2番目のu1ビットのデータが得られたことになり、乱数系列としては全部でu1×2ビットのデータが得られたことになる。

【0074】以降、ステップS6、S7、S3、S4の処理ループを1回繰り返すごとに、順次、u1ビットの乱数が生成されていく。そして、ステップS4に必要な長さの乱数系列が得られた場合に、ステップS5でループを抜けて、処理を終了する。

【0075】以上により、第1の線形フィードバックシフトレジスタ20により生成された乱数系列を、第2の線形フィードバックシフトレジスタ22により生成された乱数系列に基づいて順序変更したものが得られる。

【0076】以下では、本乱数生成装置の動作について具体例を用いて説明する。ここでは、u2=3とし、第2の線形フィードバックシフトレジスタ20により生成された乱数が直接、記憶装置24のアドレスを示すものとする。

【0077】また、第1の線形フィードバックシフトレジスタ20により、乱数系列“ABCDEFGH I J K L M N…”が生成され、第2の線形フィードバックシフトレジスタ22により、乱数系列“011001011111000010…”が生成されるものとする。

【0078】ここで、A～Nの各々は、2値の乱数系列を先頭からu1ビット毎に区切って得たデータを表すものとする。u2=3とするので、図5に示すように第2の線形フィードバックシフトレジスタ20により生成された乱数系列を3ビットごとに区切って得られる“011”、“001”、“011”、“111”、“000”、“010”、…が、この順番に記憶装置24にアドレス入力として与えられることになる。

【0079】動作前においては図6(a)のように記憶装置24のアドレス000～111には有効なデータが格納されていない状態である。まず、 $m=2^{u2}=2^3=8$ であるので、ステップS1において初期状態がセットされた後、ステップS2において、第1の線形フィードバックシフトレジスタ20により、乱数系列“ABCDEFGH”が生成され、図6(b)のように記憶装置24のアドレス000～111にされる。

【0080】次に、ステップS3にて第2の線形フィードバックシフトレジスタ22により“011”が生成され、ステップS4にて記憶装置24のアドレス“01

1”の内容Dが出力される。

【0081】そして、ステップS6にて第1の線形フィードバックシフトレジスタ20により“I”が生成され、これがステップS7にて記憶装置24のアドレス“011”に格納される。このときの記憶装置24の各アドレスの内容を図6(c)に示す。

【0082】次に、ステップS3に戻り、第2の線形フィードバックシフトレジスタ22により“001”が生成され、ステップS4にて記憶装置24のアドレス“001”の内容Bが出力される。

【0083】そして、ステップS6にて第1の線形フィードバックシフトレジスタ20により“J”が生成され、これがステップS7にて記憶装置24のアドレス“001”に格納される。このときの記憶装置24の各アドレスの内容を図6(d)に示す。

【0084】さらに同様の処理を4回繰り返すと、乱数系列“DBIHAC”が得られる。この間の記憶装置24の各アドレスの内容の遷移を図7(a)～(d)に示す。

【0085】以上の処理を必要回数繰り返すことにより、所望の長さの乱数系列を得ることができる。ここで、図8(a)と(b)に、第1の線形フィードバックシフトレジスタ20により生成された乱数系列と、本乱数生成装置により生成された乱数系列を対象する形で示す。

【0086】図8に示されるように、第2の線形フィードバックシフトレジスタ22により生成された乱数系列に基づいて、第1の線形フィードバックシフトレジスタ20により生成された乱数系列が、u1ビット単位で順序変更されて、本乱数生成装置から出力されていることがわかる。

【0087】なお、本乱数生成装置は、図2を用いて説明した暗号装置および復号装置における乱数系列(鍵系列)を生成するための乱数生成装置として用いると効果的である。この場合、線形フィードバックシフトレジスタ20の初期状態および線形フィードバックシフトレジスタ22の初期状態の組そのものまたはこれらを特定可能な識別子が共通鍵として用いられる。

【0088】このような本実施形態によれば、記憶装置を緩衝域として用いることで、装置規模に比して線形複雑度が大きく、暗号的にも安全な乱数生成装置、あるいはこれを有する加算型ストリーム暗号の暗号装置および復号装置を実現することができる。

【0089】また、装置規模に比して線形複雑度が大きいことは、安価に安全な暗号装置および復号装置を構築できることを意味する。ここで、本実施形態の第1および第2の線形フィードバックシフトレジスタのレジスタ長を各々LA、LBとすると、本乱数生成装置での線形複雑度は、ほぼ

$$LA \times 2^{LB}$$

である。

【0090】なお、乱数生成装置の他の構成例として、第1の線形フィードバックシフトレジスタ20および第2の線形フィードバックシフトレジスタ22の少なくとも一方を、他の公知の乱数生成装置（例えば、複数の線形フィードバックシフトレジスタの出力を非線形コンバイナで結合するもの、線形フィードバックシフトレジスタの出力に非線形変換を施すもの、あるいは加算ジェネレータ（summation generator）など）に置き換えた構成も考えられる。これを図2の暗号装置および復号装置に適用する場合にも、もちろん、置き換えた乱数生成装置の初期状態そのものまたはこれを特定可能な識別子が共通鍵として用いられる。

【0091】また、図9に示すように、乱数生成装置のさらに他の構成例として、第1の線形フィードバックシフトレジスタ20と第2の線形フィードバックシフトレジスタ22とを1つの線形フィードバックシフトレジスタ26として共通化しても良い。この場合、第1の線形フィードバックシフトレジスタ20としてu1ビットの乱数を生成する動作と、第2の線形フィードバックシフトレジスタ22としてu2ビットの乱数を生成する動作とを交互に行えば良い。さらに、この場合においても、線形フィードバックシフトレジスタ26を、他の公知の乱数生成装置に置き換えた構成も考えられる。

【0092】また、線形フィードバックシフトレジスタから出力される乱数系列を単に並べ変えるだけであれば、例えば、線形フィードバックシフトレジスタから出力される乱数系列を適当な長さによって、一旦バッファ装置に蓄積し、この適当な長さの乱数系列をランダムに並べ変えて出力する方法も考えられるが、この場合、線形フィードバックシフトレジスタでの乱数生成と順番のバッファ装置における並べ変えから出力までの各処理がバッチ的に行われるので、遅延が生じる欠点がある。これに対して、本実施形態によれば、線形フィードバックシフトレジスタでの乱数生成とバッファ装置からの出力が短いサイクルで繰り返されるので、遅延が生じないという効果を得ることもできる。

【0093】図10に、本発明の他の実施形態に係る乱数生成装置の構成を示す。また、図11に、本乱数生成装置の動作の流れを示す。本乱数生成装置は、第1の線形フィードバックシフトレジスタ30、第2の線形フィードバックシフトレジスタ32、第1の記憶装置34、第1の記憶装置36、非線形コンバイナ38を備えている。

【0094】本乱数生成装置は、先の実施形態で図3を参照しながら説明した乱数生成装置を2組用意し、それらから得られる2つの乱数系列に非線形変換処理を施したものを出力するものに相当する。ただし、図10では、線形フィードバックシフトレジスタを各機能専用に4個すべて設けず、併用することで2個だけ設けたもの

となっている。

【0095】すなわち、第1の線形フィードバックシフトレジスタ30および第2の線形フィードバックシフトレジスタ32の基本的な構成は、先の実施形態で図3を参照しながら説明した第1の線形フィードバックシフトレジスタ20および第2の線形フィードバックシフトレジスタ22と同様である。相違するのは、第1の線形フィードバックシフトレジスタ30を第1の記憶装置34へのデータ入力と第2の記憶装置36へのアドレス入力の両方に使用し、第2の線形フィードバックシフトレジスタ32を第2の記憶装置36へのデータ入力と第1の記憶装置34へのアドレス入力の両方に使用する点である。

【0096】本実施形態では、第1の線形フィードバックシフトレジスタ30により生成され第1の記憶装置34へのデータ入力となる乱数D1と、第2の線形フィードバックシフトレジスタ32により生成され第2の記憶装置36へのデータ入力となる乱数D2とは、同じビット長でも良いし、異なるビット長でも良い。

【0097】また、第1の線形フィードバックシフトレジスタ30により生成され第2の記憶装置36へのアドレス入力となる乱数A1と、第2の線形フィードバックシフトレジスタ32により生成され第1の記憶装置34へのアドレス入力となる乱数A2とは、同じビット長でも良いし、異なるビット長でも良い。

【0098】ようするに、本実施形態では、第1の線形フィードバックシフトレジスタ30は、初期処理のために第1の記憶装置34に格納すべき必要個数の乱数を生成した後は、第2の記憶装置36へのアドレス入力となる乱数A1と、第1の記憶装置34へのデータ入力となる乱数D1とを交互に生成し、同様に、第2の線形フィードバックシフトレジスタ32は、初期処理のために第2の記憶装置36に格納すべき必要個数の乱数を生成した後は、第1の記憶装置34へのアドレス入力となる乱数A2と、第2の記憶装置36へのデータ入力となる乱数D2とを交互に生成する。

【0099】第1の記憶装置34および第2の記憶装置36の構成は、先の実施形態で図3を参照しながら説明した記憶装置24と同様である。非線形コンバイナ38の機能は、例えば、2入力1出力の非線形関数fである。非線形コンバイナ38としては、公知のものを使用することができる（例えば文献1参照）。

【0100】また、非線形コンバイナ38は、2つの入力データの各ビットの値をもとにした組み合わせ回路で実現しても良い。なお、線形フィードバックシフトレジスタの初期状態や、記憶装置のアドレス入力となる乱数と該乱数により示されるアドレスとの関係についても、先に説明したものと同様である。

【0101】次に、図11を参照しながら本乱数生成装置の動作について説明する。まず、初期処理として、第

1の線形フィードバックシフトレジスタ20および第2の線形フィードバックシフトレジスタ22夫々を所望の初期状態にセットする(ステップS11)。

【0102】そして、第1の線形フィードバックシフトレジスタ30により所定ビットの乱数を所定個数生成し、これらを第1の記憶装置34に格納するとともに、第2の線形フィードバックシフトレジスタ32により所定ビットの乱数を所定個数生成し、これらを第2の記憶装置36に格納する(ステップS12)。

【0103】次に、第1の線形フィードバックシフトレジスタ30によりアドレス用の乱数A1を1つ生成するとともに、第2の線形フィードバックシフトレジスタ32によりアドレス用の乱数A2を1つ生成する。(ステップS13)。

【0104】そして、第1の記憶装置34のアドレスのうち、ステップS13で生成された乱数A2にて示されるアドレスの内容を出力するとともに、第2の記憶装置36のアドレスのうち、ステップS13で生成された乱数A1にて示されるアドレスの内容を出力する(ステップS14)。

【0105】さらに、非線形コンバイナ38により、ステップS14にて第1の記憶装置34および第2の記憶装置36夫々から出力されたデータをもとにした所定の被線形変換処理を実行して、得られたデータを出力する(ステップS15)。

【0106】この時点で、生成すべき乱数系列のうち最初の所定ビット分のデータが得られたことになる。次に、第1の線形フィードバックシフトレジスタ30によりデータ用の乱数D1を1つ生成するとともに、第2の線形フィードバックシフトレジスタ32によりデータ用の乱数D2を1つ生成する(ステップS17)。

【0107】そして、第1の記憶装置34のアドレスのうち、ステップS14で内容の出力されたアドレスに、ステップS17で生成された乱数D1を格納するとともに、第2の記憶装置36のアドレスのうち、ステップS14で内容の出力されたアドレスに、ステップS17で生成された乱数D2を格納する(ステップS18)。

【0108】次に、ステップS13に戻って上記と同様に乱数A1とA2を生成し(ステップS13)、各記憶装置24、26において乱数A2、A1にて示されるアドレスの内容を夫々出力し(ステップS14)、この2つの出力をもとにした所定の被線形変換処理により得られたデータを出力する(ステップS15)。

【0109】この時点で、生成すべき乱数系列のうち2番目の所定ビットのデータが得られたことになる。以降、ステップS17、S18、S13、S14、S15の処理ループを1回繰り返すごとに、順次、所定ビットの乱数が生成されていく。

【0110】そして、ステップS15で必要な長さの乱数系列が得られた場合に、ステップS16でループを抜

けて、処理を終了する。なお、本乱数生成装置は、図2を用いて説明した暗号装置および復号装置における乱数系列(鍵系列)を生成するための乱数生成装置として用いると効果的である。この場合、線形フィードバックシフトレジスタ30の初期状態および線形フィードバックシフトレジスタ32の初期状態の組そのものまたはこれらを特定可能な識別子が共通鍵として用いられる。

【0111】このような本実施形態によれば、記憶装置を緩衝域として用いることで、装置規模に比して線形複雑度が大きく、暗号的にも安全な乱数生成装置、あるいはこれを有する加算型ストリーム暗号の暗号装置および復号装置を実現することができる。

【0112】また、装置規模に比して線形複雑度が大きいことは、安価に安全な暗号装置および復号装置を構築できることを意味する。ここで、本実施形態の第1および第2の線形フィードバックシフトレジスタのレジスタ長を各々LA、LBとすると、本乱数生成装置での線形複雑度は、ほぼ

$$2^{LA} \times 2^{LB}$$

である。

【0113】なお、乱数生成装置のさらに他の構成例として、第1の線形フィードバックシフトレジスタ30と第2の線形フィードバックシフトレジスタ32とを1つの線形フィードバックシフトレジスタとして共通化しても良い。

【0114】あるいは、その逆に、第1の線形フィードバックシフトレジスタ30および第2の線形フィードバックシフトレジスタ32の少なくとも一方を、データ用とアドレス用に分離し、装置全体として3つあるいは4つの線形フィードバックシフトレジスタを設けた構成にすることも可能である。

【0115】また、上記した線形フィードバックシフトレジスタを1、2、3、または4個備えた構成において、少なくとも1つの線形フィードバックシフトレジスタを、他の公知の乱数生成装置(例えば、複数の線形フィードバックシフトレジスタの出力を非線形コンバイナで結合するもの、線形フィードバックシフトレジスタの出力に非線形変換を施すもの、あるいは加算ジェネレータ(summation generator)など)に置き換えた構成も考えられる。これを図2の暗号装置および復号装置に適用する場合にも、もちろん、置き換えた乱数生成装置の初期状態そのものまたはこれを特定可能な識別子が共通鍵として用いられる。

【0116】図12に、本発明のさらに他の実施形態に係る乱数生成装置の構成を示す。また、図11に、本乱数生成装置の動作の流れを示す。本実施形態は、図3の線形フィードバックシフトレジスタの部分、図3の乱数生成装置自体で置き換えて、構成を階層化したものである。

【0117】図12の他にも、図10の線形フィードバ

ックシフトレジスタの部分、図10の乱数生成装置自体で置き換えた構成も考えられる。あるいは、図3の線形フィードバックシフトレジスタの部分、図10の乱数生成装置自体で置き換えた構成や、図10の線形フィードバックシフトレジスタの部分、図3の乱数生成装置自体で置き換えた構成も考えられる。

【0118】その他、種々の構成が考えられる。また、図12ように2階層の構造にとどまらず、3階層以上に階層化した乱数生成装置、例えば図12における線形フィードバックシフトレジスタの部分、さらに図3の乱数生成装置あるいは図12の乱数生成装置で置き換えた構成など、種々のものが考えられる。

【0119】また、以上の各機能は、ソフトウェアとしても実現可能である。また、上記した各手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体として実施することもできる。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0120】

【発明の効果】本発明に係る乱数生成装置や方法によれば、記憶装置を緩衝域として用いることで、少ない装置規模で大きな線形複雑度を達成することができる。従って、本発明に係る乱数生成装置や方法を適用することにより、経済的かつ安全なストリーム暗号を実現することができる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係る乱数生成装置の構成を示す図

【図2】本発明の実施の形態に係る乱数生成装置を用い

た暗号システムの一例を示す図

【図3】本発明の一実施形態に係る乱数生成装置の構成を示す図

【図4】同実施形態に係る乱数生成装置の動作を示すフローチャート

【図5】生成されたアドレス系列を示す図

【図6】記憶装置の内容の遷移を示す図

【図7】記憶装置の内容の遷移を示す図

【図8】変換前後の乱数系列を示す図

【図9】同実施形態に係る乱数生成装置の変形例の構成を示す図

【図10】本発明の他の実施形態に係る乱数生成装置の構成を示す図

【図11】同実施形態に係る乱数生成装置の動作を示すフローチャート

【図12】本発明のさらに他の実施形態に係る乱数生成装置の構成を示す図

【図13】線形フィードバックシフトレジスタの構成例を示す図

【図14】他の乱数生成装置の構成例を示す図

【符号の説明】

2, 4, 40, 42…乱数生成部

6…乱数変換部

10a, 10b…乱数生成装置

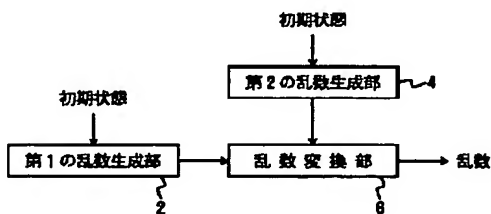
12a, 12b…論理演算処理装置

20, 22, 26, 30, 32…線形フィードバックシフトレジスタ

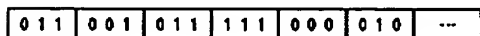
24, 34, 36…記憶装置

38…非線形コンバイナ

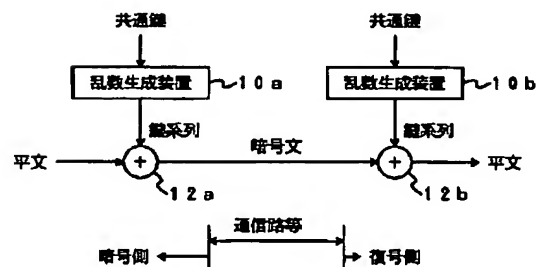
【図1】



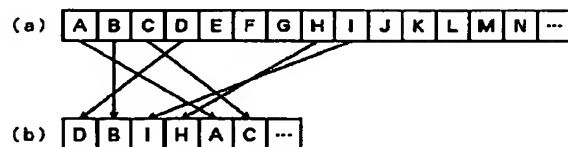
【図5】



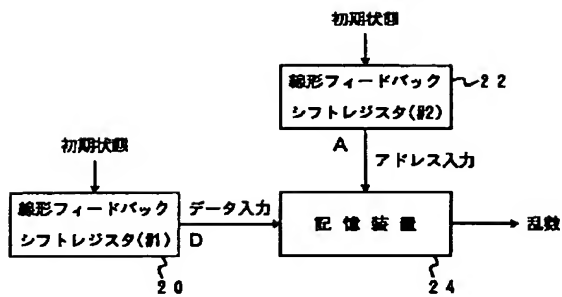
【図2】



【図8】



【図3】



【図6】

| アドレス | 内容 |
|------|----|
| 000 | |
| 001 | |
| 010 | |
| 011 | |
| 100 | |
| 101 | |
| 110 | |
| 111 | |

(a)

| アドレス | 内容 |
|------|----|
| 000 | A |
| 001 | B |
| 010 | C |
| 011 | D |
| 100 | E |
| 101 | F |
| 110 | G |
| 111 | H |

(b)

【図7】

| アドレス | 内容 |
|------|----|
| 000 | A |
| 001 | J |
| 010 | C |
| 011 | K |
| 100 | E |
| 101 | F |
| 110 | G |
| 111 | H |

(a)

| アドレス | 内容 |
|------|----|
| 000 | A |
| 001 | J |
| 010 | C |
| 011 | K |
| 100 | E |
| 101 | F |
| 110 | G |
| 111 | L |

(b)

| アドレス | 内容 |
|------|----|
| 000 | A |
| 001 | B |
| 010 | C |
| 011 | I |
| 100 | E |
| 101 | F |
| 110 | G |
| 111 | H |

(c)

| アドレス | 内容 |
|------|----|
| 000 | A |
| 001 | J |
| 010 | C |
| 011 | I |
| 100 | E |
| 101 | F |
| 110 | G |
| 111 | H |

(d)

【図9】

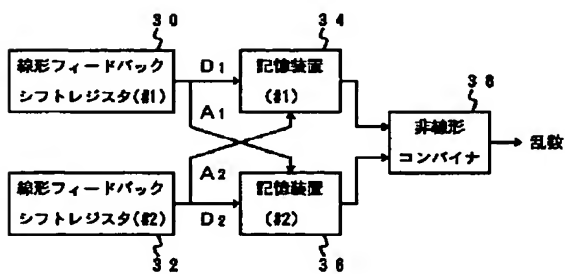
| アドレス | 内容 |
|------|----|
| 000 | M |
| 001 | J |
| 010 | C |
| 011 | K |
| 100 | E |
| 101 | F |
| 110 | G |
| 111 | L |

(c)

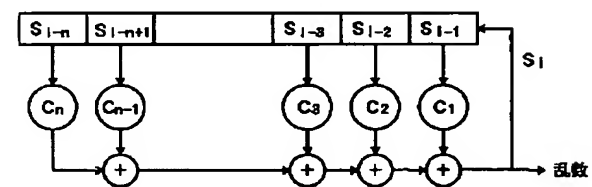
| アドレス | 内容 |
|------|----|
| 000 | M |
| 001 | B |
| 010 | N |
| 011 | D |
| 100 | E |
| 101 | F |
| 110 | G |
| 111 | H |

(d)

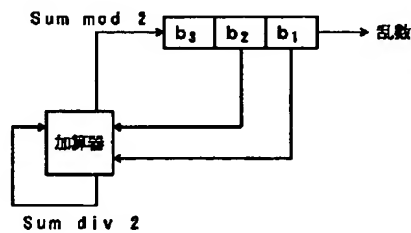
【図10】



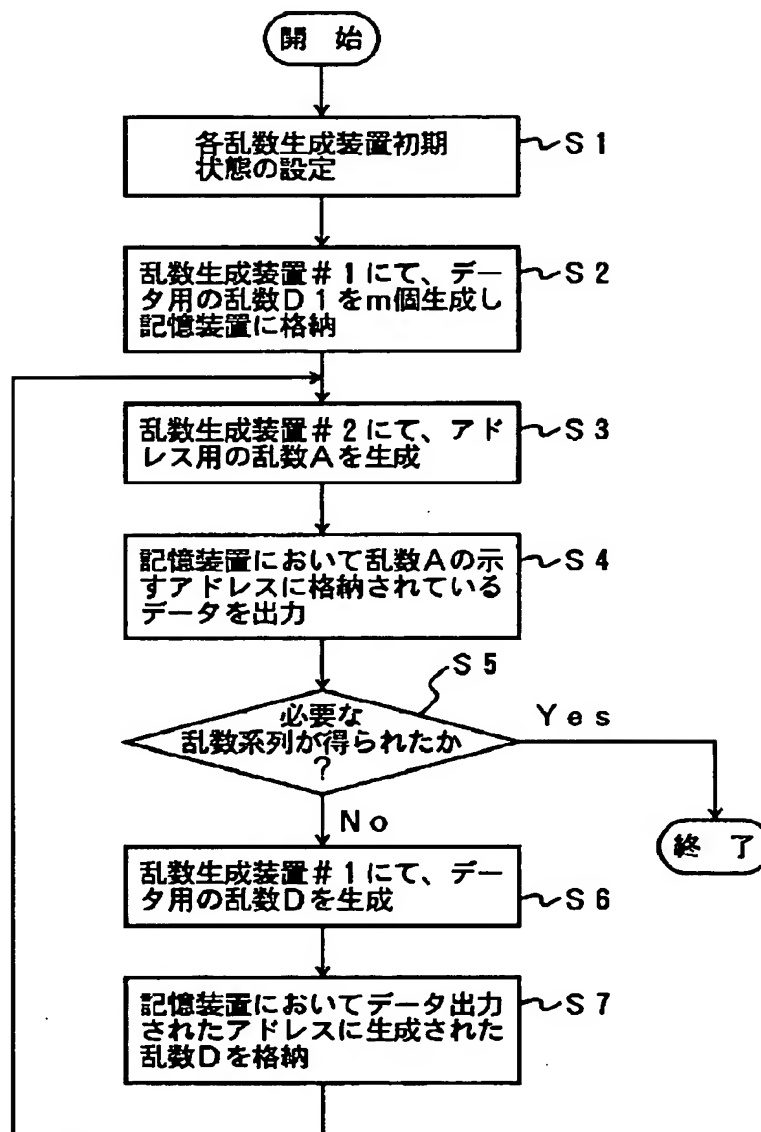
【図13】



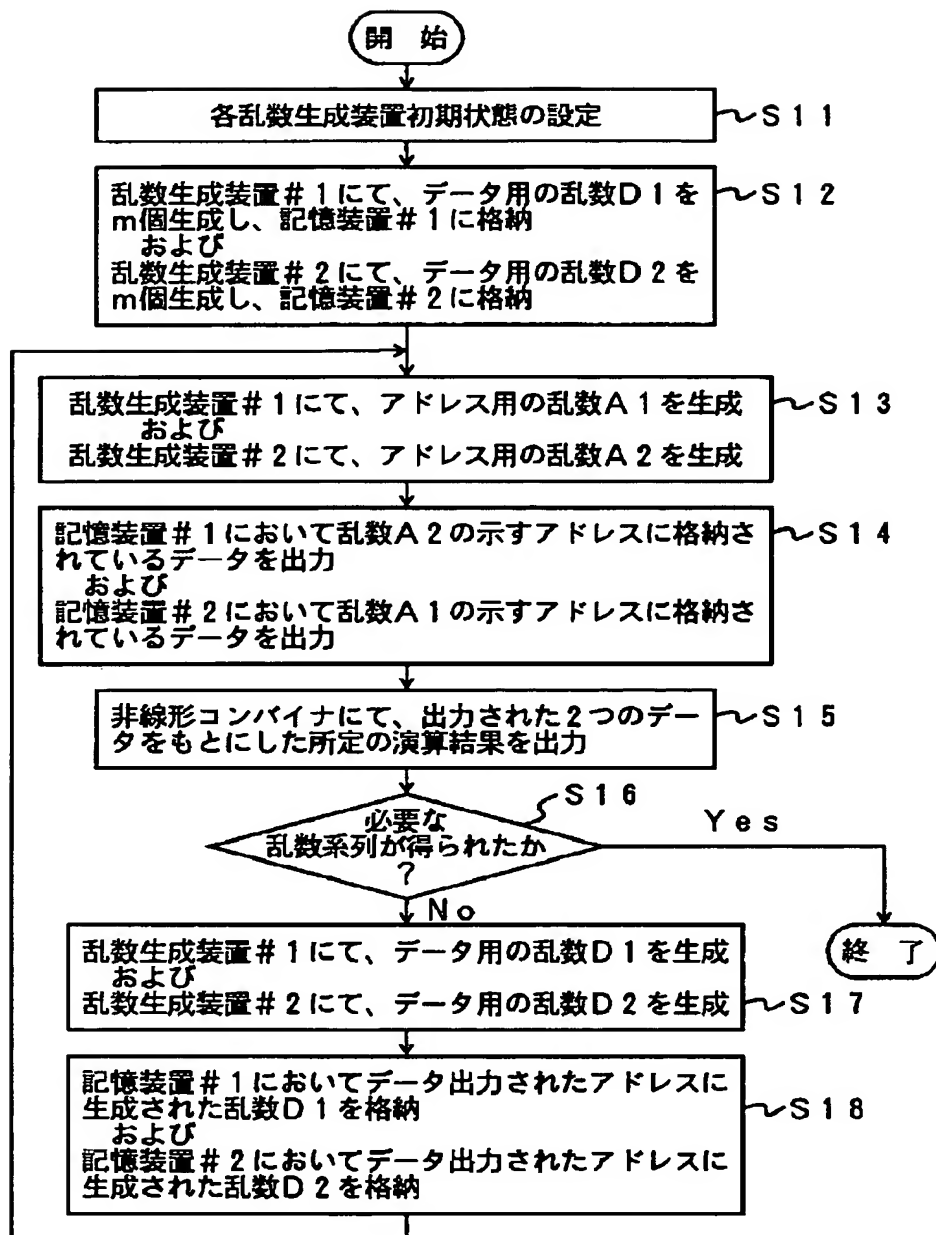
【図14】



【図4】



【図11】



【図12】

